UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/800,173	03/06/2001	Peter V. Radatti	E-2538	3615

7590 04/13/2006

John F.A. Earley III
86 The Commons at Valley Forge East
1288 Valley Forge Road
P.O.Box 750
Valley Forge, PA 19482-0750

EXAMINER	
YIGDALL, MICHAEL J	

ART UNIT	PAPER NUMBER
2192	

DATE MAILED: 04/13/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	09/800,173	RADATTI, PETER V.	
	Examiner	Art Unit	
	Michael J. Yigdall	2192	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *23 January 2006*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *4,8-15 and 18-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *4,8-15 and 18-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on January 23, 2006 has been entered. Claims 4, 8-15 and 18-21 are pending.

Response to Arguments

2. Applicant's arguments have been fully considered but they are not persuasive.

Applicant contends that Pedrizetti does not include the elements recited in the claims because Pedrizetti discloses a second comparison that is not recited in the claims (remarks, page 6, last paragraph to page 7, first full paragraph).

However, the plain language of the claims does not exclude Pedrizetti. Notwithstanding the possibility of hash collisions, Pedrizetti teaches the elements recited in the claims, as set forth below. Moreover, it is noted that claims 8 and 21 each recite two transmission steps and two comparison steps, which is analogous to Applicant's characterization of the reference.

In response to Applicant's arguments about the new limitation added to the claims that "a second cryptographic hash [is] installed on said target," it is noted that Applicant construes this language to mean a second cryptographic hash that preexists on the target, rather than a second cryptographic hash that is generated during the course of operation (remarks, page 7, last paragraph to page 8, second full paragraph).

However, as Applicant notes, Pedrizetti and McGuire each disclose a second hash that is generated at the client. A reasonable interpretation is that in both references, the second hash is "installed on" the client because it exists only on the client and is never transmitted to the client from the server. Nonetheless, the arguments are moot in view of the new ground(s) of rejection, as set forth below with reference to Heath.

Applicant implies that Pedrizetti and McGuire cannot be combined without destroying the invention of Pedrizetti (remarks, page 8, third full paragraph).

However, the examiner does not agree with Applicant's assumptions. Pedrizetti applies a hash function to generate the bit table (see, for example, column 1, lines 45-48). The goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11). McGuire teaches a cryptographic hash function that, in fact, generates unique hash values (see, for example, column 9, lines 9-16). There is no evidence to suggest that substituting Pedrizetti's hash function with a cryptographic hash function would somehow destroy the invention. On the contrary, the cryptographic hash function would satisfy Pedrizetti's goal of generating hash values that are as unique as possible. Applying a cryptographic hash function may reduce or even eliminate the possibility of hash collisions in Pedrizetti, and this would not change the invention's principle of operation, nor would it render the invention unsatisfactory for its intended purpose.

Applicant suggests that Pedrizetti teaches away from the combination (remarks, page 8, last paragraph to page 9, top).

However, this argument is not compelling. As Applicant notes, Pedrizetti intends to minimize the amount of data transmitted to and from the client. McGuire's goal is the same (see, for example, column 7, lines 24-56). Pedrizetti transmits the hash values to the client in the form of a compressed bit table (see, for example, column 4, lines 51-58), and in view of McGuire, these hash values would be generated with a cryptographic hash function.

3. The rejection of claims 4 and 8-21 under 35 U.S.C. 112, first paragraph, is withdrawn in view of Applicant's argument that, while the specification does not define "cryptographic hash," a cryptographic hash is inherently "comprised of a unique data identifier" such as recited in the claims (remarks, page 5).

Response to Amendment

4. The rejection of claims 8-21 under 35 U.S.C. 101 is withdrawn in view of Applicant's amendment.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 4 and 8-15 and 18-21 are rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Patent No. 6,151,708 to Pedrizetti et al. (art of record, "Pedrizetti") in view of U.S.

Patent No. 6,493,871 to McGuire et al. (art of record, "McGuire") in view of U.S. Patent No. 6,006,034 to Heath et al. (now made of record, "Heath").

With respect to claim 4 (currently amended), Pedrizetti discloses an apparatus for transmitting data to a target (see, for example, the abstract) comprising:

(a) a means for updating, present on a distribution media, and further comprising data, data information and a first hash of said data information (see, for example, FIG. 1 and column 1, lines 41-65, which shows a system for updating software from a distribution server, comprising update data, information based on the update, and a hash table based on the information);

(b) a means for transmission between said distribution media and said target (see, for example, pathway 104 in FIG. 1 and column 2, lines 57-61, which shows a means for transmission between the server and client);

(c) a means for obtaining data information from said distribution media (see, for example, column 1, lines 52-56, which shows that update data information is obtained by the client from the distribution server); and

(d) a means for processing said first hash of said data information (see, for example, FIG. 5 and associated text, and column 1, lines 48-59, which shows that the client processes the information to determine the availability of updates);

whereby said means for obtaining data information from said distribution media obtains said first hash from said means for updating present on said distribution media, which first hash is transmitted through said means for transmission to said means for processing, and which upon receipt of said hash of said data information compares said first hash to a second hash installed

on said target in order to determine if said data should be transmitted to said target (see, for example, column 1, lines 48-59, which shows that the hash table and the update data information is transferred to the client for processing and is compared to a second hash table on the client to determine whether or not the actual update data should be transferred as well).

Although Pedrizetti discloses a first hash that is transmitted to the client and a second hash on the client, as presented above (also see, for example, column 4, lines 51-58), Pedrizetti does not expressly disclose the limitation that the first and second hashes are cryptographic hashes and the limitation that the first cryptographic hash is comprised of a unique data identifier.

However, McGuire teaches a similar apparatus for transmitting data to a target (see, for example, the abstract), including a cryptographic hash of data information that uniquely identifies and distinguishes different versions of a file (see, for example, column 9, lines 9-16). McGuire discloses comparing the cryptographic hash so as to exclude unneeded files (see, for example, column 9, lines 32-38) and minimize the amount of data transmitted to the target (see, for example, column 7, lines 24-56).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti such that the first and second hashes are cryptographic hashes and the first hash is comprised of a unique data identifier, such as taught by McGuire, so as to minimize the amount of data transmitted to the client. Furthermore, the goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11), and McGuire teaches that the cryptographic hash function generates unique hash values (see, for example, column 9, lines 9-16).

Although Pedrizetti discloses that the second hash exists on the target (see, for example, column 5, lines 8-11), Pedrizetti does not expressly disclose the limitation that the second cryptographic hash is installed on the target.

However, Heath teaches a similar apparatus for transmitting data to a target (see, for example, the abstract), including a cryptographic digest or hash (see, for example, column 5, lines 7-11) that is stored at or installed on the target (see, for example, column 5, lines 64-67), so as to enable the target to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the apparatus of Pedrizetti and McGuire such that the second cryptographic hash is installed on the target, such as taught by Heath, so as to periodically and automatically obtain updates as needed.

With respect to claim 8 (currently amended), Pedrizetti discloses a computer-implemented method for transmitting data to a target (see, for example, the abstract) comprising the steps of:

(a) transmitting a first hash of data information from a first distribution media to said target (see, for example, column 1, lines 45-49, which shows that a hash table based on the update data information is transferred to the client from the distribution server);

(b) comparing said first hash to a second hash installed on said target in order to determine if data information should be transmitted to said target (see, for example, column 1, lines 49-56, which shows that the hash table is compared to a second hash table on the client to determine whether or not additional information should be transferred as well);

(c) transmitting said data information from a second distribution media, if necessary, to said target (see, for example, column 1, lines 52-56, which shows that update data information is transferred to the client if needed; also see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a second distribution media, may be used);

(d) comparing said data information with said target in order to determine if said data should be transmitted to said target (see, for example, column 1, lines 52-59, which shows that the update data information is compared with the client to determine whether or not the actual update data should be transferred as well).

Although Pedrizetti discloses a first hash that is transmitted to the client and a second hash on the client, as presented above (also see, for example, column 4, lines 51-58), Pedrizetti does not expressly disclose the limitation that the first and second hashes are a cryptographic hashes and the limitation that the first cryptographic hash is comprised of a unique data identifier.

However, McGuire teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic hash of data information that uniquely identifies and distinguishes different versions of a file (see, for example, column 9, lines 9-16). McGuire discloses comparing the cryptographic hash so as to exclude unneeded files (see, for example, column 9, lines 32-38) and minimize the amount of data transmitted to the target (see, for example, column 7, lines 24-56).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti such that the hash is a cryptographic hash comprised of a unique data identifier, such as taught by McGuire, so as to minimize the amount

of data transmitted to the client. Furthermore, the goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11), and McGuire teaches that the cryptographic hash function generates unique hash values (see, for example, column 9, lines 9-16).

Although Pedrizetti discloses that the second hash exists on the target (see, for example, column 5, lines 8-11), Pedrizetti does not expressly disclose the limitation that the second cryptographic hash is installed on the target.

However, Heath teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic digest or hash (see, for example, column 5, lines 7-11) that is stored at or installed on the target (see, for example, column 5, lines 64-67), so as to enable the target to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti and McGuire such that the second cryptographic hash is installed on the target, such as taught by Heath, so as to periodically and automatically obtain updates as needed.

With respect to claim 9 (currently amended), the rejection of claim 8 is incorporated, and Pedrizetti further discloses obtaining data information from said second distribution media (see, for example, column 1, lines 52-56, which shows that update data information is obtained by the client from the distribution server).

With respect to claim 10 (currently amended), the rejection of claim 9 is incorporated, and Pedrizetti further discloses the limitation wherein obtaining data information from said second distribution media further comprises using an http address to obtain data information (see, for example, column 2, lines 61-65, which shows that an Internet connection may be used in conjunction with a Web browser for the software update system; also see, for example, FIG. 6A, which shows a Web browser using an HTTP address).

With respect to claim 11 (currently amended), the rejection of claim 8 is incorporated, and Pedrizetti further discloses the limitation wherein the first and second distribution media are the same (see, for example, server 100 in FIG. 1, which shows the software update system using a single server).

With respect to claim 12 (currently amended), the rejection of claim 8 is incorporated, and Pedrizetti further discloses the limitation wherein either the first and second distribution media at least partially comprises a network (see, for example, column 2, lines 57-58, which shows a server in communication with a client over a communications pathway, i.e. in a network).

With respect to claim 13 (currently amended), the rejection of claim 8 is incorporated, and Pedrizetti further discloses preparing said data information from attributes of said data (see, for example, column 5, lines 50-60, which shows an index file having update data information based on attributes of the actual update data, such as version number and package name; note that the step of preparing the index file is inherent to the method).

With respect to claim 14 (currently amended), the rejection of claim 13 is incorporated, and Pedrizetti further discloses the limitation wherein said data comprises one or more software product data files (see, for example, column 1, lines 41-45, which shows that software program updates are transferred from the distribution server to the client).

With respect to claim 15 (currently amended), the rejection of claim 13 is incorporated, and Pedrizetti further discloses preparing said cryptographic hash from said data information (see, for example, column 1, lines 45-48, which shows a hash table prepared from the update data information).

With respect to claim 18 (currently amended), the rejection of claim 8 is incorporated, and Pedrizetti further discloses transmitting said data from a third distribution media to said target (see, for example, column 1, lines 56-59, which shows that update data is transferred to the client from the distribution server; also see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a third distribution media, may be used).

With respect to claim 19 (currently amended), the rejection of claim 18 is incorporated, and Pedrizetti further discloses the limitation wherein the third distribution media at least partially comprises a network (see, for example, column 2, lines 57-58, which shows a server in communication with a client over a communications pathway, i.e. in a network).

With respect to claim 20 (currently amended), the rejection of claim 19 is incorporated, and Pedrizetti further discloses editing data on said target in order to update data on said target

(see, for example, column 3, lines 29-41, which shows that data on the client is edited and updated).

With respect to claim 21 (currently amended), Pedrizetti discloses a computer-implemented method for transmitting data to a target (see, for example, the abstract) comprising the steps of:

(a) providing a software product (see, for example, column 1, lines 41-45, which shows that software program updates are provided on a server);

(b) preparing data information about said software product (see, for example, column 5, lines 50-60, which shows an index file having information based on the software update; note that the step of preparing the index file is inherent to the system);

(c) preparing a first hash of data information about said software product (see, for example, column 1, lines 45-48, which shows a hash table prepared from the update data information);

(d) storing said software product on a first distribution media (see, for example, update data 114 in FIG. 1, which shows the software program update data stored on a server);

(e) storing said data information on a second distribution media (see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a second distribution media, may be used for storage);

(f) storing said first hash of data information on a third distribution media (see, for example, column 6, lines 14-17, which shows that a third-party server, i.e. a third distribution media, may be used for storage);

(g) transmitting said hash of data information to said target (see, for example, column 1, lines 45-49, which shows that a hash table based on the update data information is transferred to the client);

(h) comparing said first hash to a second hash installed on said target in order to determine if data information should be transmitted to said target (see, for example, column 1, lines 49-56, which shows that the hash table is compared to a second hash table on the client to determine whether or not additional information should be transferred as well);

(i) transmitting said data information, if necessary, to said target (see, for example, column 1, lines 52-56, which shows that update data information is transferred to the client if needed);

(j) comparing said data information with said target in order to determine if said data should be transmitted to said target (see, for example, column 1, lines 52-59, which shows that the update data information is compared with the client to determine whether or not the actual update data should be transferred as well);

(k) transmitting said data, if necessary, to said target (see, for example, column 1, lines 56-59, which shows that update data is transferred to the client if needed); and

(l) editing said data on said target in order to update data on said target (see, for example, column 3, lines 29-41, which shows that data on the client is edited and updated).

Although Pedrizetti discloses a first hash that is transmitted to the client and a second hash on the client, as presented above (also see, for example, column 4, lines 51-58), Pedrizetti does not expressly disclose the limitation that the first and second hashes are a cryptographic

hashes and the limitation that the first cryptographic hash is comprised of a unique data identifier.

However, McGuire teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic hash of data information that uniquely identifies and distinguishes different versions of a file (see, for example, column 9, lines 9-16). McGuire discloses comparing the cryptographic hash so as to exclude unneeded files (see, for example, column 9, lines 32-38) and minimize the amount of data transmitted to the target (see, for example, column 7, lines 24-56).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti such that the hash is a cryptographic hash comprised of a unique data identifier, such as taught by McGuire, so as to minimize the amount of data transmitted to the client. Furthermore, the goal of Pedrizetti's hash function is to generate hash values that are as unique as possible (see, for example, column 11, lines 3-11), and McGuire teaches that the cryptographic hash function generates unique hash values (see, for example, column 9, lines 9-16).

Although Pedrizetti discloses that the second hash exists on the target (see, for example, column 5, lines 8-11), Pedrizetti does not expressly disclose the limitation that the second cryptographic hash is installed on the target.

However, Heath teaches a similar method for transmitting data to a target (see, for example, the abstract), including a cryptographic digest or hash (see, for example, column 5, lines 7-11) that is stored at or installed on the target (see, for example, column 5, lines 64-67), so

as to enable the target to periodically and automatically obtain updates as needed (see, for example, column 2, lines 46-62).

It would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Pedrizetti and McGuire such that the second cryptographic hash is installed on the target, such as taught by Heath, so as to periodically and automatically obtain updates as needed.

Conclusion

7. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Yigdall whose telephone number is (571) 272-3707. The examiner can normally be reached on Monday through Friday from 7:30am to 4:00pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Tuan Q. Dam can be reached on (571) 272-3695. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MY

Michael J. Yigdall
Examiner
Art Unit 2192

mjy

Chameli C. Das
CHAMELI C. DAS
PRIMARY EXAMINER
7/11/06